IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
Before the Board of Patent Appeals and Interferences

Applicant	: B. Royer
Serial No.	: 09/817,324
Filed	: March 26, 2001
For	: A SYSTEM AND USER INTERFACE FOR MANAGING USER ACCESS TO NETWORK COMPATIBLE APPLICATIONS
Examiner	: Zachary A. Davis
Art Unit	: 2137

APPEAL BRIEF

May It Please The Honorable Board:

Appellants appeal the Final Rejection, dated January 13, 2006, of Claims 1 - 23 of the above-identified application. The fee of five hundred dollars ($500.00) for filing this Brief and any associated extension fee is to be charged to Deposit Account No. 19-2179. Enclosed is a single copy of this Brief.

Please charge any additional fee or credit any overpayment to the above-identified Deposit Account.

Appellants do not request an oral hearing.

I. REAL PARTY IN INTEREST

The real party in interest of Application Serial No. 09/817,324 is the Assignee of record:

Siemens Medical Solutions Health Services Corporation
51 Valley Stream Parkway
Malvern, PA 19355-1406

II. RELATED APPEALS AND INTERFERENCES

There is currently a co-pending appeal in related application serial number 09/817,322 wherein a Notice of Appeal has been filed on June 5, 2006. The present application and the application of the co-pending appeal claim priority from the same Provisional Application Serial No. 60/261,148.

A Notice of Appeal was filed in application serial number 09/817,320 on August 15, 2005 and as a result, prosecution was re-opened by Non-Final Office Action on March 9, 2006 followed by a subsequent Notice of Appeal on April 12, 2006. A Request for Continued Examination with a Preliminary Amendment was filed in response thereto on June 12, 2006.

A Notice of Appeal was filed in application serial number 09/817,323 on July 7, 2005 and as a result, prosecution was re-opened by Non-Final Office Action on March 9, 2006. A response to the Non Final Office Action was filed on June 7, 2006.

The present application and application serial numbers 09/817,323 and 09/817,320 claim priority from the same provisional application serial number 60/261,148.

III. STATUS OF THE CLAIMS

Claims 1 – 23 are rejected and the rejection of claims 1 – 23 is appealed.

IV. STATUS OF AMENDMENTS

All amendments were entered and are reflected in the claims included in Appendix I.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Independent claim 1 provides a system used by a first application for managing user access to at least one of a plurality of network compatible applications (page 1, line 36 to page 2, line 1). An authentication processor receives user identification information including a user identifier and initiates authentication of the user identification information using an authentication service (page 2, lines 1-3; Figure 2, 220). At least one communication processor communicates an authentication service identifier and corresponding user identifier to a managing application (page 2, lines 3-6; Figure 2, 250). The authentication service identifier identifies an authentication service used to authenticate identification information of the corresponding user (page 2, lines 6-7; Figure 2, 220). Application specific context information in a data field of a URL is automatically communicated separately from session identification information, to a second application of the plurality of network compatible applications in response to a user command to initiate execution of the second application and in response to authentication of the user identification information (page 5, lines 25-37; Figure 2, 200, 230, 250). The application specific context information supports acquisition from the second application of information associated with a current operational context of the first application (page 5, lines 33-35; Figure 2, 250).

Independent claim 2 provides a system used by a first application for managing user access to at least one of a plurality of network compatible applications (page 1, line 36 to page 2, line 1). An authentication processor receives user identification information including a user identifier and initiates authentication of the user identification information using an authentication service (page 2, lines 1-3; Figure 2, 220). At least one communication processor communicates an authentication service identifier and a corresponding user identifier to a managing application (page 2, lines 3-6; Figure 2, 250). The authentication service identifier identifies an authentication service used to authenticate identification information of the corresponding user (page 2, lines 6-7; Figure 2, 220). The at least one communication processor also automatically communicates application specific context information in a data field of a URL to a second application of the plurality of network compatible applications in response to a user command to initiate execution of the second application and in response to authentication of the user identification information (page 5, lines 25-37; Figure 2, 200, 230, 250). The application specific context information comprises at least one of, (a) a user identifier and (b) a patient identifier (page 10, lines 35-37; Figure 2, 207; Figure 5, 517). A communication processor of the at least one communication processor encrypts an address portion of the URL and incorporates the encrypted address portion of the URL, together with the address portion of the URL in non-encrypted form, into a single processed URL data string (page 11, lines 35-page 13, line 24; Figure 5, 530).

Dependent claim 4 includes the features of independent claim 1 along with the additional feature that a communication processor of the at least one communication processor communicates the authentication service identifier and the corresponding user identifier to a managing application for compilation of a database (page 18, lines 6-7; Figure 7, 703, 705).

Independent claim 6 provides a system used for processing user access to network compatible applications (page 1, line 36 to page 2, line 1). An authentication processor receives an authentication service identifier and corresponding user identifier data pairs from at least one of a plurality of applications, compiles a database using the data pairs, and maps a non-authenticated user identifier of a second application to an authenticated different user identifier of a first application using the database (page 2, lines 1-2 and 8-10; Figure 2, 220). At least one communication processor communicates the authenticated different user identifier to the second application and automatically communicates application specific context information in a data field of a URL separately from session identification information, to the second application in response to a user command to initiate execution of the second application (page 5, lines 25-27; Figure 2, 200, 230, 250). The application specific context information supports acquisition from the second application of information associated with a current operational context of the first application (page 5, lines 33-35; Figure 2, 250).

Dependent claim 7 includes the features of independent claim 6 along with the additional feature that the authentication service identifier identifies an authentication service used to authenticate identification information comprising a user identifier of the corresponding user to provide an authenticated user identifier (page 17, lines 28-33; Figure 5, 500, 517).

Dependent claim 8 includes the features of independent claim 6 along with the additional feature that the authentication processor performs the mapping using the database by matching an authentication service identifier of the second application with an authentication service identifier of the first application and providing the authenticated different user identifier of the first application as a mapped user identifier (page 17, line 37 to page 18, line 7; Figure 7, 700, 703, 305; Figure 2, 200, 250).

Dependent claim 11 includes the features of independent claim 6 along with the additional feature that a communication processor of the at least one communication processor communicates a parameter to the second application. The parameter identifies success or failure of the mapping (page 18, line 18-20; Figure 8, 809).

Independent claim 14 provides a system used for processing user access to Internet compatible applications (page 4, lines 3-5). An authentication processor receives an authentication service identifier and corresponding user identifier from a parent application and maps a non-authenticated user identifier of a child application to an authenticated different user identifier of the parent application (page 2, lines 8-10; Figure 2, 220, 203). At least one communication processor communicates the authenticated different user identifier to the child application and automatically communicates application specific context information in a data field of a URL separately from session identification information, to the child application in response to a user command to initiate execution of the child application and in response to communicating the authenticated different user identifier (page 5, lines 25-37; Figure 2, 200, 230, 250). The application specific context information supports acquisition from the child application of information associated with a current operational context of the parent application (page 5, lines 33-35; Figure 2, 250).

Independent claim 21 provides a method used for processing user access to Internet compatible applications (page 4, lines 3-5). An authentication service identifier and corresponding user identifier are received form a parent application (page 2, lines 1-2; Figure 2, 220). A non-authenticated user identifier of a child application is mapped to an authenticated different user identifier of the parent application (page 2, lines 8-10; Figure 2, 220). The authenticated different user identifier is communicated to the child application (page 7, lines 8-9; Figure 2, 250, 200, 224; Figure 5, 520). Application specific context information in a data field of a URL is automatically communicated, separately from session identification information, to the child application in response to a user command to initiate execution of the child application and in response to communicating the authenticated different user identifier (page 5, lines 25-37; Figure 2, 200, 250, 226; Figure 10, 445, 449, 450, 453). The application specific context information supports acquisition from the child application of information associated with a current operational context of the parent application (page 5, lines 33-35; Figure 2, 250).

Independent claim 23 provides a method used by a first application for managing user access to at least one of a plurality of network compatible applications (page 1, line 36 to page 2, line 1). User identification information including a user identifier is received (page 2, lines 1-2; Figure 2, 220). Authentication of the user identification information using an authentication service is initiated (page 2, lines 1-3; Figure 2, 220). An authentication service identifier and a corresponding user identifier are communicated to a managing application (page 2, lines 4-6; Figure 2, 220, 250). The authentication service identifier identifies an authentication service used to authenticate identification information of the corresponding user (page 2, lines 6-7; Figure 2, 220). Application specific context information in a data field of a URL is automatically communicated separately from session identification information, to a second application of the plurality of network compatible applications in response to a user command to initiate execution of the second application and in response to authentication of the user identification information (page 5, lines 25-37; Figure 2, 200, 230, 250). The application specific context information supports acquisition from the second application of information associated with a current operational context of the first application (page 5, lines 33-35; Figure 2, 250).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Cohen et al. (U.S. Patent 6,178,511) in view of Levergood et al. (U.S. Patent 5,708,780).

Claims 1 and 3-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cohen et al. (U.S. Patent 6,178,511) in view of Levergood et al. (U.S. Patent 5,708,780) and De la Huerga et al. (U.S. Patent 5,903,889).

VII. ARGUMENTS

Cohen in view of Levergood does not make claim 2 unpatentable. Thus, reversal of the rejection of claim 2 under 35 U.S.C. § 103(a) is respectfully requested. Moreover, Cohen in view of Levergood and De la Huerga does not make claims 1 and 3-23 unpatentable. Thus, reversal of the Final Rejection (hereinafter termed "rejection") of claims 1 and 3-23 under 35 U.S.C. § 103(a) is respectfully requested.

Overview of the Cited References

Cohen describes a single sign-on mechanism to enable a user to access a target application on a target resource in a distributed computer enterprise. One or more configuration directives each identifying a given logon process and any associated methods required to access the target application on the target resource are stored in a preferably global-accessible database (CIM). For each of a set of users, a preferably global-accessible database (PKM) stores user-specific and application-specific information enabling the user to access and logon to one or more target resources. During a particular session, a logon coordinator (LC) mechanism coordinates given user information with the configuration directive to enable the given user information with the configuration directive to enable the given user to perform a given action with respect to the target application without specifying the given logon process and the application-specific information (see Abstract).

Levergood describes a method for controlling and monitoring access to network servers. The process includes client-server sessions over the Internet involving hypertext files. In the hypertext environment, a client views a document transmitted by a content server with a standard program known as the browser. Each hypertext document or page contains links to other hypertext pages which the user may select to traverse. When the user selects a link that is directed to an access-controlled file, the server subjects the request to a secondary server which determines whether the client has an authorization or valid account. Upon such verification, the user is provided with a session identification which allows the user to access the requested file as well as any other files within the present protected domain (see Abstract).

De la Huerga describes a system for retrieving, modifying and collecting data records having a plurality of formats and distributed on a plurality of databases on a computer network. The system includes means for detecting various types, relationships, and classifications of data records and modifying them accordingly to support interactive, hypertext-linked display of, and organized access to, the data records. The system further includes means to store a related set of data records on a mass storage device such as a CD-ROM to provide non-network access to the data records. Adapted for use in a hospital environment, the invention facilitates access by care providers, administrators, and insurance company agents to a patient's cumulative, and possibly extensive, record (see Abstract)

Rejection of Claim 2 under 35 U.S.C. 103(a) over Cohen (U.S. Patent 6,178,511) in view of Levergood (U.S. Patent 5,708,870)

Cohen in view of Levergood does not make claim 2 unpatentable. Thus, reversal of the Final Rejection (hereinafter termed "rejection") of claim 2 under 35 U.S.C. § 103(a) is respectfully requested.

In rejecting claims under 35 U.S.C. § 103, it is incumbent upon the examiner to establish a factual basis to support the legal conclusion of obviousness. *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596, 1598 (Fed.Cir. 1988). In so doing, the Examiner is expected to make the factual determinations set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 17, 148 USPQ 459, 467 (CCPA 1966), and to provide a reason why one having ordinary skill in the pertinent art would have been led to modify the prior art or to combine prior art references to arrive at the claimed invention. Such reason must stem from some teaching, suggestion, or implication in the prior art as a whole or knowledge generally available to one having ordinary skill in the art. *Uniroyal, Inc. v. Rudkin-Wiley Corp.*, 837 F.2d 1044, 1051, 5 USPQ2d 1434, 1438 (Fed.Cir. 1988), *cert. denied*, 488 U.S. 825 (1988); *Ashland Oil Inc. v. Delta Resins & Refractories, Inc.*, 776 F.2d 28, 293, 227 USPQ 657, 664 (Fed.Cir. 1985), *cert. denied*, 475 U.S. 1017 (1986); *ACS Hosp. Sys., Inc. v. Montefiore Hosp.*, 732 F.2d 1572, 1577, 221 USPQ 929, 933 (Fed.Cir. 1984). These showings by the Examiner are an essential part of complying with the burden of presenting a *prima facie* case of obviousness. *In re Oetiker*, 977 F.2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed.Cir. 1992).

CLAIM 2

Independent claim 2 includes "automatically communicating application specific context information in a data field of a URL to a second application of said plurality of network compatible applications in response to authentication of said user identification information." Thereby the system enables a user to logon and authenticate with a first application such as a patient census application and gain automatic access to multiple other applications such as a medical laboratory test result application and in response to user authentication with the test result application, be automatically provided with desired test results for the specific patient selected in the first patient administration application (see example described on Application page 5 lines 8-12 and elsewhere in connection with Figure 2). This is done without the user having to re-enter context information (e.g., a patient identifier) by another command following automatic authentication with a second application. This capability is not shown or suggested in Cohen with Levergood. The combination, in the present claimed invention, of automatic authentication to multiple applications together with automatic communication of application specific context information "in response to a user command to initiate execution of said second application and in response to authentication of said user identification information" facilitates user friendly operation and user seamless navigation in a plurality of concurrently operating applications. The system addresses the problems involved in "facilitating user initiation (e.g., logon), operation and termination (e.g., logoff) of multiple Internet applications and in securely passing URL, patient (and user) identification and other information between applications. A managing application is employed to coordinate user operation sessions. Specifically, the managing application coordinates inactivity timeout operation and maintains and conveys properties between concurrent applications in order to **create a smooth user operation session**" (Application page 4 lines 23-31).

The Rejection on page 9 recognizes that Cohen does not disclose "automatically" communicating "application specific **context** information" in "a data field of a URL" to a "second application of said plurality of network compatible applications" in "response to authentication of said user identification information" initiated by the "authentication processor". However, Levergood (with Cohen) in column 4 lines 1-18, column 6, lines 36-42 relied on in the Rejection on page 9 also fails to show or suggest "automatically" communicating "application specific **context** information" (such as a patient identifier) in "a data field of a URL" to a "second application of said plurality of network compatible applications" in "response to authentication of said user identification information" initiated by the "authentication processor". Levergood discloses appending session identification information (SID) to a URL (column 3 line 39) and as indicated in the Rejection, the Levergood SID may incorporate a user identifier (Column 5 lines 56-60). However, the Levergood SID is used for authentication and determining access to documents ("a user is provided with a session identification which allows the user to access to the requested file as well as any other files within the present protection domain" - Levergood Abstract).

Consequently, Levergood with Cohen cannot "automatically" communicate "application specific **context** information" (such as a patient identifier) in "a data field of a URL" to a "second application of said plurality of network compatible applications" in "**response to authentication** of said user identification information". Since the context information relied on in the Rejection is within the SID used to authenticate user access to data it cannot be "automatically" communicated in "**response to authentication"**. Further, the Levergood SID is not "application specific **context** information," as recited in the present claimed invention since it is within the SID used for the entirely different purpose of authentication.

Applicant further respectfully submits "[t]he **session** context information comprises a **session** identifier, a hash value, and application specific data" (Application page 5, lines

28-29). "**Session** context information" is not equivalent to "**application specific** context information." A "session identifier" identifies a session of computer operation including one or more executable applications (a "session identifier is used by applications 200 and 230 to identify a user initiated session in communicating with manager 250" – Application page 5 lines 29-32, "Specifically the managing application coordinates inactivity timeout operation and maintains and conveys properties between concurrent applications in order to create a smooth user operation session" (Application page 4 lines 27-30). This is corroborated in Levergood (a "user is provided with a session identification which allows the user to access the requested file as well as any other files within the present protection domain" - Levergood Abstract). Therefore, "session identification information" is NOT (and is not suggested by) a "date 712 and time 716" associated with requested report data accessed via a URL or a "report designator 718" e.g., name or other identifier of the report accessed. Further, session identification information is not "application specific **context** information." Though Levergood discloses appending session identification information (SID) to a URL (column 3 line 39, and column 6, lines 22-24), session identification is used for authentication and determining access to documents (a user is provided with a session identification which allows the user to access the requested file as well as any other files within the present protection domain" - Levergood Abstract). Session identification information is not "application specific **context** information" as recited in the present claimed invention.

As admitted on page 9 of the rejection, Cohen (with Levergood) does NOT discuss or suggest the claimed features of "automatically communicating application specific **context** information in a data field of a URL" such as a patient identifier "to a second application of said plurality of network compatible applications" "in response to authentication of said user identification information" in combination with facilitating automatic authentication to multiple network compatible applications" by "communicating an authentication service identifier" and a "corresponding user identifier to a **managing application**" as recited in the present invention. As further admitted on page 9 of the rejection, Cohen (with Levergood) also fails to show or suggest the claimed features of encrypting an "**address portion** of said URL link" to the "second application" and incorporating the "encrypted address portion of said URL, together with said address portion of said URL in non-encrypted form, into a single processed URL data string" as recited in the present claimed invention. In an exemplary embodiment of the invention illustrated in the Application specification pages 11-12, application 200 advantageously, for example, encrypts "a **URL** link **address portion**" comprising a hash value identified by field identifier "GSH=" derived by "hashing on the **addressable portion** of a fully qualified URL" comprising the "URL data either lying between the "http://" and the question mark "?" or from the data lying between the "http://" and the pound/number sign "#" - whichever comes first" (Application page 9 lines 35-37 and page 11 line 25). Consequently, in the exemplary URL string shown processed in the specification page 12

www.smed.com/altoona/prd/results.exe/1?GSM=16253384937&GSH=24017&Pid=1772693&Frgclr=blue

the compressed address portion is 24017 which is concatenated with a patient identifier (Application page 12 line lines 15-20) as shown:

GSH=24017&Pid=1772693

and is encrypted into the string

16sfdjwhejeyw7rh3hekw

to produce the processed URL including the encrypted URL address portion:

www.smed.com/altoona/prd/results.exe/1?GSM=16253384937:16sfdjwhejeyw7rh3hekw&Frgclr=blue.

This is an exemplary "processed URL".

Applicant respectfully submits that these features are also neither disclosed nor suggested in Levergood. The Rejection makes a **fundamental error** on page 9 in interpreting the Levergood reference. Contrary to the Rejection statements on page 9, Levergood in column 5 lines 56-65 and column 3 lines 34-37 relied on in the Rejection merely discloses encryption of a session identifier (SID) and an IP address. Specifically, Levergood states "the digital signature is a cryptographic hash of the remaining items in the SID and the authorized IP address which are encrypted with a secret key which is shared by the authentication and content servers" (Levergood column 5 lines 61-65, also see column 3 lines 33-37). This is unlike the present claimed invention wherein "a communication processor…encrypts an address portion of said URL and incorporates said encrypted address portion of said URL, together with said address portion of said URL in non-encrypted form, into a single processed URL data string."

Further, although in Levergood a valid session identifier "typically comprises" an "accessible domain" in the "SID encrypted with a secret key", the Levergood accessible domain is NOT a URL or an address portion of a URL (Levergood column 3 lines 33-37). Levergood explicitly defines an accessible "domain" as a collection of files and NOT a

URL or address portion of a URL ("A protection domain is **defined** by the service provider and is a **collection of controlled files** of common protection within one or more servers" – Levergood column 3 lines 52-55). This is further made clear in column 5 lines 54-61 stating a "preferred SID is a sixteen character ASCII string that encodes **96** bits of SID data" that contains "an **8**-bit **domain** comprising **a set of information files** to which the current SID authorizes access". Such an "accessible domain" as used by Levergood is not in a URL link address portion. This is further corroborated in Levergood in column 6 lines 29-34 indicating that such a domain is in the non-address, URL data field portion of a URL (e.g. after the question mark), specifically, a "REDIRECT URL might be: "http://auth.com/authenticate?**domain**= [domain]& URL = http://content.com/report".

Levergood does not show or suggest encrypting an "**address portion** of said URL link" to the "second application" and incorporating the "encrypted address portion of said URL, together with said address portion of said URL in non-encrypted form, into a single processed URL data string". Neither a session identifier nor an IP address as used in Levergood are a "URL or a URL address portion". Indeed a URL and IP address are distinct and different objects with totally different functions ("the content server records the URL **and** the IP address" – Levergood column 5 lines 37-38). An IP address describes an electronic address of an Internet entity whereas a URL "consists of three parts: the transfer format, the host name of the machine that holds the file, and the **path** to the file" (Levergood column 2 lines 28-31). A session identifier identifies a user session of computer operation for example and is itself a distinct entity that may be conveyed within a field of a URL (Application page 11 line 17). The claimed "address portion" is NOT (and is NOT suggested by) the "SID" or "IP address" of Levergood. Levergood does not encrypt an address portion of a URL.

The Rejection states in the Response to Arguments section on page 7 that if the domain includes a collection of files within a server, then the "domain must include an identification and/or address for these files", thus the domain can indeed include an address portion of a URL. However, nowhere in Levergood et al. is it disclosed or suggested that the domain includes a URL or even a portion of a URL. In fact, Levergood et al. explicitly defines a protection domain as "a collection of controlled files of common protection within one or more servers" in column 3, lines 52-55. The Examiner's reliance on interpreting "a collection of files" to anticipate "using a received encryption key to encrypt a URL link address portion" is a **fundamental error.** In so doing, the Examiner is not only engaging in the pure speculation that the Levergood "collection of files" has something to do with a URL, but also that it leads to teaching encryption of a "URL address portion" as specifically defined in the present Application. Further, this speculation is without foundation and **directly contradicts** Levergood's own teaching in column 5 line 59 that a domain is an 8 – bit value ("SID data" contains "an **8**-bit **domain** comprising **a set of information files")**. Thus, Levergood et al. neither disclose nor suggest "a URL processor for adaptively processing a URL link" as in the present claimed invention.

Applicant respectfully submits that there is no reason, problem recognition or motivation for Levergood to provide the features of the present claimed invention. The purpose of Levergood, on the other hand is to provide encryption that ensures validity of session identifiers (SIDs) by using an "Internet server" to subject "the client to an authorization routine prior to issuing the SID" (Levergood column 3 lines 24-26). In contrast, the Application addresses the problem of preventing "URL replay or redirection" through its recognition that URLs are "vulnerable to corruption" (Application page 11 lines 1-9).

Applicant further respectfully submits that there is no reason or motivation to combine the systems disclosed by Cohen and Levergood. Levergood and Cohen are mutually incompatible systems, including different URL format and security management features respectively which either cannot be reconciled or for which there is no described method of reconciliation, and thus cannot be combined to create an operable system. Additionally, Cohen describes password-mapping and encryption as problematic, which is in direct conflict with the encryption system of Levergood (Cohen col. 1, lines 45-63). Thus, the combination of Cohen with Levergood would produce an inoperable system and neither discloses nor suggests the claimed arrangement.

Therefore, if one were able to combine Cohen with Levergood to produce an operable system, Applicant respectfully submits that a combination of Cohen with Levergood would produce a system that provides a single sign-on mechanism that ensures validity of session identifiers. This combination neither discloses nor suggests "automatically communicating application specific context information in a data field of a URL to a second application of said plurality of network compatible applications in response to a user command to initiate execution of said second application and in response to authentication of said user identification information" as recited in the present claimed invention. Further, this combination neither discloses nor suggests "at least one communication processor encrypts an address portion of said URL and incorporates said encrypted address portion of said URL, together with said address portion of said URL in non-encrypted form, into a single processed URL data string" as recited in the present claimed invention. Consequently, withdrawal of the rejection of claim 2 under 35 USC 103(a) is respectfully requested.

Rejection of Claims 1 and 3-23 under 35 U.S.C. 103(a) over Cohen (U.S. Patent 6,178,511) in view of Levergood (U.S. Patent 5,708,870) and De la Huerga (U.S. Patent 5,903,889)

CLAIMS 1 and 3

The system of claim 1 includes "automatically communicating **application specific context** information in a **data field of a URL** separately from session identification information, to a second application of said plurality of network compatible applications in response to a user command to initiate execution of said second application and in response to authentication of said user identification information". Such application specific context information includes a patient identifier or user identifier, for example (Application page 10 lines 35-37). The claimed system advantageously "automatically" communicates "**application specific context** information in a data field of a URL **separately** from session identification information, to a second application of said plurality of network compatible applications" such as a patient identifier "in response to authentication of said user identification information" initiated by the "authentication processor". Further, the "application specific context information" supports "acquisition" from the "second application of information associated with a current operational context of said first application".

Thereby the system enables a user to logon and authenticate with a first application such as a patient census application and gain automatic access to multiple other applications such as a medical laboratory test result application and in response to user authentication with the test result application, be automatically provided with desired test results for the specific patient selected in the first patient administration application (see example described on Application page 5 lines 8-12 and elsewhere in connection with Figure 2). This is done without the user having to re-enter context information (e.g., a patient identifier) by another command following automatic authentication with a second application. This capability is not shown or suggested in Cohen with Levergood and De la Huerga. The combination of automatic authentication to multiple applications together with automatic communication of application specific context information "in response to a user command to initiate execution of said second application and in response to authentication of said user identification information" facilitates user friendly operation and user seamless navigation in a plurality of concurrently operating applications. The system addresses the problems involved in "facilitating user initiation (e.g., logon), operation and termination (e.g., logoff) of multiple Internet applications and in securely passing URL, patient (and user) identification and other information between applications. A managing application is employed to coordinate user operation sessions. Specifically, the managing application coordinates inactivity timeout operation and maintains and conveys properties between concurrent applications in order to **create a smooth user operation session**" (Application page 4 lines 23-31).

The Rejection on page 10 recognizes that Cohen does not disclose the claimed features of "automatically communicating application specific **context** information in a data field of a URL" to a "second application of said plurality of network compatible applications" "in response to authentication of said user identification information" initiated by the "authentication processor". However, Levergood (with Cohen) in column 4 lines 1-18, column 6, lines 58-66 and column 7, lines 15-21 relied on in the Rejection on pages 2-3 and 10 also fails to show or suggest "automatically" communicating "application specific **context** information" (such as a patient identifier) in "a data field of a URL" to a "second application of said plurality of network compatible applications" in "response to authentication of said user identification information" initiated by the "authentication processor". Levergood discloses appending session identification information (SID) to a

URL (column 3 line 39) and as indicated in the Rejection, the Levergood SID may incorporate a user identifier (Column 5 lines 56-60). However, the Levergood SID is used for authentication and determining access to documents ("a user is provided with a session identification which allows the user to access to the requested file as well as any other files within the present protection domain" - Levergood Abstract).

Consequently, Levergood with Cohen cannot "automatically" communicate "application specific **context** information" (such as a patient identifier) in "a data field of a URL" to a "second application of said plurality of network compatible applications" in "**response to authentication** of said user identification information". Since the context information relied on in the Rejection is within the SID used to authenticate user access to data it cannot be "automatically" communicated in "**response to authentication**". Further, the Levergood SID is not "application specific **context** information," as recited in the present claimed invention and does NOT support "acquisition from said second application of information associated with a current operational context of said first application" as recited in the present claimed invention, since it is within the SID used for the entirely different purpose of authentication.

As recognized in the Rejection on page 11, Levergood with Cohen fails to show or suggest "automatically" communicating "application specific **context** information" (such as a patient identifier) in "a data field of a URL **separately from session** identification information". However, contrary to the Rejection statement on page 11, De la Huerga (with or without Levergood and Cohen) also does not show or suggest "automatically" communicating "application specific **context** information" in "a data field of a URL **separately from session** identification information" as recited in the present claimed invention. De la Huerga in column 10 lines 43-59 and Figure 14A shows a URL conveying "application specific **context** information" (a patient identifier) in "a data field of a URL" but does NOT show or suggest a URL conveying **"session** identification information" in a separate data field of the URL. The items relied on in the Rejection in De la Huerga column 10 lines 43-59 have nothing to do with a computer "session" and De la Huerga nowhere even mentions or contemplates "session". De la Huerga column 10 lines 43-59 states "Embedded in this URL address 700 is information regarding the type of data 704, the patient's identification 708, the date 712 and time 716 of the data requested, and a report designator 718". The "date 712 and time 716 of the data requested" are the time and date associated with a report accessed via the URL and have nothing to do with a computer "session". Similarly, "report designator 718" is a designator, e.g., name or other identifier of the report accessed. The Rejection allegation on page 11 that items 712, 716 and 718 have anything to do with a computer "session" is erroneous, unfounded speculation. These items provide no 35 USC 112 compliant enabling disclosure of "automatically" communicating "application specific **context** information" in "a data field of a URL **separately from session** identification information".

Applicant further respectfully submits that the comment in the response to arguments section of the rejection on page 3 **mis-reads** page 5, lines 28-29 of the Application. "The **session** context information comprises a **session** identifier, a hash value, and application specific data" (page 5, lines 28-29). "**Session** context information" is not equivalent to "**application specific** context information." A "session identifier" identifies a session of computer operation including one or more executable applications (a "session identifier is used by applications 200 and 230 to identify a user initiated session in communicating with manager 250" – Application page 5 lines 29-32, "Specifically the managing application coordinates inactivity timeout operation and maintains and conveys properties between concurrent applications in order to create a smooth user operation session" Application page 4 lines 27-30). This is corroborated in Levergood (a "user is provided with a session identification which allows the user access to the requested file as well as any other files within the present protection domain" - Levergood Abstract). Therefore, "session identification information" is NOT (and is not suggested by) a "date 712 and time 716" associated with requested report data accessed via a URL or a "report designator 718" e.g., name or other identifier of the report accessed. Further, session identification information is not "application specific **context** information" and does NOT support "acquisition from said second application of information associated with a current operational context of said first application". Though Levergood discloses appending session identification information (SID) to a URL (column 3 line 39, and column 6, lines 22-24), session identification is used for authentication and determining access to documents (a user is provided with a session identification which allows the user to access to the requested file as well as any other files within the present protection domain" - Levergood Abstract). Session identification information is not "application specific **context** information" and does NOT support "acquisition from said second application of information associated with a current operational context of said first application". Cohen with Levergood and De la Huerga also does not suggest the automatic feature combination comprising "automatically" communicating "application specific context information" in "a data field of a URL separately from session identification information" together with facilitating automatic authentication to multiple network compatible applications" by "communicating an authentication service identifier" and a "corresponding user identifier to a **managing application**". This provides seamless navigation advantages not shown or suggested in the combined references.

Applicant further respectfully submits that there is no reason or motivation to combine the systems disclosed by De la Huerga, Cohen and Levergood. In fact, Levergood and De la Huerga are mutually incompatible systems as De la Huerga provides no 35 USC 112 compliant enabling disclosure of "session" information as required for proper operation of the Levergood system. Therefore, a combination of Levergood with De La Huerga would result in an inoperable system. Additionally, Cohen describes password-mapping and encryption as problematic, which is in direct conflict with the encryption system of Levergood (Cohen col. 1, lines 45-63). Thus, the combination of Cohen with Levergood would similarly produce an inoperable system and neither discloses nor suggests the claimed arrangement..

Furthermore, even if Cohen, Levergood and De la Huerga were able to be combined to produce an operable system, Applicant respectfully submits that incorporating the De la Huerga features in Cohen with Levergood as suggested in the Rejection results in the system burden of requiring a user to initiate at least a second command (e.g., a URL link selection) conveying application specific context information to an Application **in addition to** initiating a first command conveying session identification information (e.g., a URL link selection) to the Application. These references, in any combination, neither disclose nor suggest the use of a single command to seamlessly achieve this navigation, as described in the present claimed invention. Further the absence of any common problem recognition, advantage identification or other motivation in the three references undermines any suggestion that combining these disparate systems would be obvious to one of ordinary skill in the art. Further, the Rejection fails to provide any showing of how such disparate systems may be combined when each system has features that conflict with systems employed by the other references (in security management, URL format, handshaking etc.).

Consequently it is respectfully submitted that the present invention as claimed in claim 1 is patentable over Cohen in view of Levergood and De la Huerga. Dependent claim

3 is considered to be patentable for the reasons given in connection with claim 1. Therefore, withdrawal of the rejection of claims 1 and 3 under 35 USC 103(a) is respectfully requested.

CLAIMS 4 and 5

Dependent claim 4 is considered to be patentable based on its dependence on claim 1. Therefore the reasons given in connection with claim 1 also apply to claim 4. Claim 4 is also considered to be patentable because Cohen with Levergood and De la Huerga does not show or suggest a system in which "a communication processor of said at least one communication processor communicates said authentication service identifier and said corresponding user identifier to a managing application for compilation of a database". Contrary to the Rejection statement on page 12, Cohen in Column 4 line 61 to column 5 line 6, lines 16-22 and 45-58 does not suggest "**compilation** of a database" including "**authentication service identifier** and said corresponding user identifier" data pairs. Cohen with Levergood and De la Huerga column 4 line 61 to column 5 line 6 recites "Preferably, PKM 24 is a secure, globally accessible repository that facilitates the single sign-on process. Although not meant to be limiting, with respect to a given user, the PKM (as will be described) preferably stores such information as a *username, a set of one or more password(s), and any other application environment-specific information such as domain name, hostname, application name, and the like*. Because this access information preferably is centralized in the PKM, users can access their target resources with one sign-on from any workstation. They can also manage their passwords from this one repository, as will also be seen". It is well understood that citation of a **general** list of items such as those italicized fail to provide 35 USC 112 compliant enabling disclosure of **specific** elements such as the recited "authentication service identifier and said corresponding user identifier" data pairs. Further, Cohen with Levergood and De la Huerga fails to show or suggest **communicating** "said authentication service identifier and said corresponding user identifier **to** a **managing application** for **compilation** of a database". In Cohen with Levergood and De la Huerga there is no suggestion, or 35 USC 112 compliant enablement of dynamic "**compilation**" of a database. There is no indication in Cohen with Levergood and De la Huerga of HOW the PKM repository is provided or any indication other than it is predefined and NOT provided by dynamic "compilation".

In view of the above remarks regarding claim 4, it is respectfully submitted that the present invention as claimed in claim 4 is patentable over Cohen in view of Levergood and De la Huerga. Dependent claim 5 is considered to be patentable for the reasons given in connection with claim 4. Therefore, withdrawal of the rejection of claims 4 and 5 under 35 USC 103(a) is respectfully requested.

CLAIMS 6, 9, 10, 12 and 13

Independent claim 6 is considered to be patentable for the reasons given in connection with claims 1, 4 and 5. Claim 6 is also considered to be patentable because Cohen with Levergood and De la Huerga does not show (or suggest) a feature combination as in claim 6 including "compiling a database" using "data pairs, mapping a non-authenticated user identifier of a second application to an authenticated different user identifier of a first application using said database" and at least one communication processor for, "automatically communicating application specific context information in a data field of a URL **separately from session** identification information, to said second application in response to a user command to initiate execution of said second application". Cohen with Levergood and De la Huerga does not show or suggest "compilation of such a database" in combination with automatically communicating application specific context information in a data field of a URL **separately** from session identification information, to said second application in response to a user command to initiate execution of said second application". Cohen with Levergood and De la Huerga also does not mention, contemplate or suggest "automatically communicating" "application specific context information supporting acquisition from said second application of information associated with a **current** operational context of said **first application**".

Applicant further respectfully submits that the comment in the response to arguments section of the rejection on page 3 **mis-reads** page 5, lines 28-29 of the Application. "The **session** context information comprises a **session** identifier, a hash value, and application specific data" (page 5, lines 28-29). "**Session** context information" is not equivalent to "**application specific** context information." As recognized on page 13 of the Rejection, Levergood with Cohen fails to show or suggest "automatically" communicating "application specific **context** information" (such as a patient identifier) in "a data field of a URL **separately from session** identification information". However, contrary to the Rejection statement on page 13, De la Huerga (with or without Levergood and Cohen) also does not show or suggest "automatically" communicating "application specific **context** information" in "a data field of a URL **separately from session** identification information". De la Huerga in column 10 lines 43-59 and Figure 14A shows a URL conveying "application specific **context** information" (a patient identifier) in "a data field of a URL" but does NOT show or suggest a URL conveying "**session** identification information" in a separate data field of the URL. The items relied on in the Rejection in De la Huerga column 10 lines 43-59 have nothing to do with a computer "session" and De la Huerga nowhere even mentions or contemplates "session". De la Huerga column 10 lines 43-59 states "Embedded in this URL address 700 is information regarding the type of data 704, the patient's identification 708, the date 712 and time 716 of the data requested, and a report designator 718". The "date 712 and time 716 of the data requested" are the time and date associated with a report accessed via the URL and having to do with a computer "session". Similarly, "report designator 718" is a designator, e.g., name or other identifier of the report accessed. The Rejection allegation on page 9 that items 712, 716 and 718 have anything to do with a computer "session" is erroneous, unfounded speculation. These items provide no 35 USC 112 compliant enabling disclosure of "automatically" communicating "application specific **context** information" in "a data field of a URL **separately from session** identification information".

A "session identifier" identifies a session of computer operation including one or more executable applications (a "session identifier is used by applications 200 and 230 to identify a user initiated session in communicating with manager 250" – Application page 5 lines 29-32, "Specifically the managing application coordinates inactivity timeout operation and maintains and conveys properties between concurrent applications in order to create a smooth user operation session." Application page 4 lines 27-30). This is corroborated in Levergood (a "user is provided with a session identification which allows the user access to the requested file as well as any other files within the present protection domain" - Levergood Abstract). Therefore, "session identification information" is NOT (and is not suggested by) a "date 712 and time 716" associated with requested report data accessed via a URL or a "report designator 718" e.g., name or other identifier of the report accessed. Further, session identification information is not "application specific **context** information" and does NOT support "acquisition from said second application of information associated with a current operational context of said first application". Though Levergood discloses appending session identification information (SID) to a URL (column 3 line 39), session identification is used for authentication and determining access to documents (a user is provided with a session identification which allows the user to access to the requested file as well as any other files within the present protection domain" -

Levergood Abstract). Session identification information is not "application specific **context** information" and does NOT support "acquisition from said second application of information associated with a current operational context of said first application". Cohen with Levergood and De la Huerga also does not suggest the automatic feature combination comprising "automatically" communicating "application specific context information" in "a data field of a URL separately from session identification information" together with facilitating automatic authentication to network compatible applications by "communicating said authenticated different user identifier to said **second application**". This provides seamless navigation advantages not shown or suggested in the combined references.

Further, Applicant respectfully submits that incorporating the De la Huerga features in Cohen with Levergood as suggested in the Rejection results in the system burden of requiring a user to initiate at least a second command (e.g., a URL link selection) conveying application specific context information to an Application **in addition to** initiating a first command conveying session identification information (e.g., a URL link selection) to the Application. These references, in any combination, neither disclose nor suggest the use of a single command to seamlessly achieve this navigation, as described in the present claimed invention. Further, the absence of any common problem recognition, advantage identification or other motivation in the three references undermines any suggestion that combining these disparate systems would be obvious to one of ordinary skill in the art. Further, the Rejection fails to provide any showing of how such disparate systems may be combined when each system has features that conflict with systems employed by the other references (in security management, URL format, handshaking etc.).

Consequently it is respectfully submitted that the present invention as claimed in claim 6 is patentable over Cohen in view of Levergood and De la Huerga. Dependent claims 9, 10, 12 and 13 are considered to be patentable for the reasons given in connection with claim 6. Therefore, withdrawal of the rejection of claims 6, 9, 10, 12 and 13 under 35 USC 103(a) is respectfully requested.

CLAIM 7

Dependent claim 7 is considered to be patentable based on its dependence on claim 6. Claim 7 is also considered to be patentable because Cohen with Levergood and De la Huerga does not show or suggest the feature combination of claim 7 in which "said authentication service identifier identifies an authentication service used to authenticate identification information comprising a user identifier of said corresponding user to provide an authenticated user identifier". Cohen's mention of "information on how to logon to the applications configured on a given machine" in column 4 lines 48-50 fails to provide 35 USC 112 compliant enabling disclosure of an "authentication service identifier" that "identifies an authentication service used to authenticate identification information comprising a user identifier of said corresponding user to provide an authenticated user identifier" in combination with the other features of this claim. Further, Cohen in column 4, line 64 to column 5, line 2 merely provides that the PKM "stores such information as a username, a set of one or more password(s), and any other application environment-specific information such as domain name, hostname, application name, and the like." Applicant further respectfully submits that a database storing the information recited in this passage of Cohen is not equivalent to an "authentication service identifier" that "identifies an authentication service used to authenticate identification information comprising a user identifier of said corresponding user to provide an authenticated user identifier" in combination with the other features of this claim. Consequently, the withdrawal of the rejection of claim 7 under 35 USC 103(a) is respectfully requested.

CLAIM 8

Dependent claim 8 is considered to be patentable based on its dependence on claim 6. Claim 8 is also considered to be patentable because Cohen with Levergood and De la Huerga does not show or suggest the feature combination of claim 8 in which "said authentication processor performs said mapping using said database by matching an authentication service identifier of said second application with an authentication service identifier of said first application and providing said authenticated different user identifier of said first application as a mapped user identifier". Cohen column 6 lines 26-37 relied on in the Rejection on page 14 merely describes that the logon coordinator gets the target systems and applications the user can signon to, the passwords and keys from the personal key manager. The system ensures that the user who logged onto the mechanism is the user who retrieves the password. This passage, and elsewhere in Cohen, fails to provide 35 USC 112 compliant enabling disclosure of an "authentication processor" that "performs said **mapping** using said database by matching an authentication service identifier of said second application with an authentication service identifier of said first application and providing said **authenticated different user identifier** of said first application as a **mapped user identifier**". These features are not specifically shown or suggested in Cohen with Levergood and De la Huerga. Consequently, the rejection of claim 8 under 35 USC 103(a) should be withdrawn.

CLAIM 11

Dependent claim 11 is considered to be patentable based on its dependence on claim 6. Claim 11 is also considered to be patentable because Cohen with Levergood and

De la Huerga does not show or suggest the feature combination of claim 11 in which "a communication processor of said at least one communication processor communicates a parameter to said second application, said parameter identifying success or failure of said mapping". The Rejection alleges this feature is shown in Cohen and relies for support on column 10 lines 35-37 ("Return codes from the interface are associated with buckets (rc. success, rc.error, etc.), allowing the appropriate action to be taken based on the bucket into which the return code falls"). However, "Return codes… allowing the appropriate action to be taken based on the bucket into which the return code falls" does not show or suggest (or provide a 35 USC 112 enabling disclosure of) communicating "a parameter to said second application…identifying success or failure of" "mapping a non-authenticated user identifier of a second application to an authenticated different user identifier of a first application using" a compiled "database". The Return codes in Cohen appear to be related to logon success (column 10 lines 22-29) and have nothing to do with success of "mapping a non-authenticated user identifier of a second application to an authenticated different user identifier of a first application using said database" in "compiling a database". As previously explained Cohen with Levergood and De la Huerga does not discuss dynamic "compilation" of such a database at all. Consequently, the rejection of claim 11 under 35 USC 103(a) should be withdrawn.

CLAIMS 14-20

Independent claim 14 is considered to be patentable for the reasons given in connection with claims 1, 4, 5 and 6. Claim 14 is also considered to be patentable because Cohen with Levergood and De la Huerga does not show (or suggest) a feature combination as in claim 14 including "mapping a non-authenticated user identifier of a child application to an authenticated different user identifier of a said parent application" and at least one communication processor for, "automatically communicating application specific context information in a data field of a URL **separately from session** identification information, to said child application in response to a user command to initiate execution of said child application and in response to communicating said authenticated different user identifier". Cohen with Levergood and De la Huerga also does not mention, contemplate or suggest "automatically communicating" "application specific context information supporting acquisition from said child application of information associated with a **current** operational context of said **parent application**".

Applicant further respectfully submits that the comment in the response to arguments section of the rejection on page 3 **mis-reads** page 5, lines 28-29 of the Application. "The **session** context information comprises a **session** identifier, a hash value, and application specific data" (page 5, lines 28-29). "**Session** context information" is not equivalent to "**application specific** context information." As recognized on page 13 of the Rejection, Levergood with Cohen fails to show or suggest "automatically" communicating "application specific **context** information" (such as a patient identifier) in "a data field of a URL **separately from session** identification information". However, contrary to the Rejection statement on page 16, De la Huerga (with or without Levergood and Cohen) also does not show or suggest "automatically" communicating "application specific **context** information" in "a data field of a URL **separately from session** identification information". De la Huerga in column 10 lines 43-59 and Figure 14A shows a URL conveying "application specific **context** information" (a patient identifier) in "a data field of a URL" but does NOT show or suggest a URL conveying "**session** identification information" in a separate data field of the URL. The items relied on in the Rejection in De la Huerga column 10 lines 43-59 have nothing to do with a computer "session" and De la Huerga nowhere even mentions or contemplates "session". De la Huerga column 10 lines 43-59 states "Embedded in this URL address 700 is information regarding the type of data

704, the patient's identification 708, the date 712 and time 716 of the data requested, and a report designator 718". The "date 712 and time 716 of the data requested" are the time and date associated with a report accessed via the URL and having to do with a computer "session". Similarly, "report designator 718" is a designator, e.g., name or other identifier of the report accessed. The Rejection allegation on page 16 that items 712, 716 and 718 have anything to do with a computer "session" is erroneous, unfounded speculation. These items provide no 35 USC 112 compliant enabling disclosure of "automatically" communicating "application specific **context** information" in "a data field of a URL **separately from session** identification information".

As described above with respect to claims 1 and 6, a "session identifier" identifies a session of computer operation including one or more executable applications (a "session identifier is used by applications 200 and 230 to identify a user initiated session in communicating with manager 250" – Application page 5 lines 29-32. "Specifically the managing application coordinates inactivity timeout operation and maintains and conveys properties between concurrent applications in order to create a smooth user operation session." Application page 4 lines 27-30). This is corroborated in Levergood (a "user is provided with a session identification which allows the user access to the requested file as well as any other files within the present protection domain" – Levergood Abstract). Therefore, "session identification information" is NOT (and is not suggested by) a "date 712 and time 716" associated with requested report data accessed via a URL or a "report designator 718" e.g., name or other identifier of the report accessed. Further, session identification information is not "application specific **context** information" and does NOT support "acquisition from said child application of information associated with a current operational context of said parent application". Though Levergood discloses appending session identification information (SID) to a URL (column 3 line 39), session identification is used for authentication and determining access to documents (a user is provided with a session identification which allows the user to access the requested file as well as any other files within the present protection domain" – Levergood Abstract). Session identification information is not "application specific **context** information" and does NOT support "acquisition from said child application of information associated with a current operational context of said parent application". Cohen with Levergood and De la Huerga also does not suggest the automatic feature combination comprising "automatically" communicating "application specific context information" in "a data field of a URL separately from session identification information" together with facilitating automatic authentication to network compatible applications by "communicating said authenticated different user identifier to said **child application**". This provides seamless navigation advantages not shown or suggested in the combined references.

Further, Applicant respectfully submits that incorporating the De la Huerga features in Cohen with Levergood as suggested in the Rejection results in the system burden of requiring a user to initiate at least a second command (e.g., a URL link selection) conveying application specific context information to an application **in addition to** initiating a first command conveying session identification information (e.g., a URL link selection) to the application. These references, in any combination, neither disclose nor suggest the use of a single command to seamlessly achieve this navigation, as described in the present claimed invention. Further the absence of any common problem recognition, advantage identification or other motivation in the three references undermines any suggestion that combining these disparate systems would be obvious to one of ordinary skill in the art. Further, the Rejection fails to provide any showing of how such disparate systems may be combined when each system has features that conflict with systems employed by the other references (in security management, URL format, handshaking etc.).

Consequently it is respectfully submitted that the present invention as claimed in claim 14 is patentable over Cohen in view of Levergood and De la Huerga. Dependent claims 15-20 are considered to be patentable for the reasons given in connection with claim 14. Therefore, withdrawal of the rejection of claims 15-20 under 35 USC 103(a) is respectfully requested.

CLAIMS 21 and 22

As stated on page 18 of the Rejection, claim 21 is a method claim that mirrors the system of claim 14. Thus the rejection argues that claim 21 is unpatentable for the same reasons given for claim 14. Applicant respectfully submits that claim 21 is in fact patentable for the reasons given above in connection with claim 14. Claim 21 is also considered to be patentable because Cohen with Levergood and De la Huerga does not show (or suggest) a feature combination as in claim 21 including "mapping a non-authenticated user identifier of a child application to an authenticated different user identifier of a said parent application" and "automatically communicating application specific context information in a data field of a URL **separately from session** identification information, to said child application in response to a user command to initiate execution of said child application and in response to communicating said authenticated different user identifier". Cohen with Levergood and De la Huerga also does not mention, contemplate or suggest "automatically communicating" "application specific context information supporting acquisition from said child application of information associated with a **current** operational context of said **parent application**".

Applicant further respectfully submits that the comment in the response to arguments section of the rejection on page 3 **mis-reads** page 5, lines 28-29 of the Application. "The **session** context information comprises a **session** identifier, a hash value, and application specific data" (page 5, lines 28-29). "**Session** context information" is not equivalent to "**application specific** context information." As recognized on page 16 of the Rejection, Levergood with Cohen fails to show or suggest "automatically" communicating "application specific **context** information" (such as a patient identifier) in "a data field of a URL **separately from session** identification information". However, contrary to the Rejection statement on page 16, De la Huerga (with or without Levergood and Cohen) also does not show or suggest "automatically" communicating "application specific **context** information" in "a data field of a URL **separately from session** identification information". De la Huerga in column 10 lines 43-59 and Figure 14A shows a URL conveying "application specific **context** information" (a patient identifier) in "a data field of a URL" but does NOT show or suggest a URL conveying "**session** identification information" in a separate data field of the URL. The items relied on in the Rejection in De la Huerga column 10 lines 43-59 have nothing to do with a computer "session" and De la Huerga nowhere even mentions or contemplates "session". De la Huerga column 10 lines 43-59 states "Embedded in this URL address 700 is information regarding the type of data 704, the patient's identification 708, the date 712 and time 716 of the data requested, and a report designator 718". The "date 712 and time 716 of the data requested" are the time and date associated with a report accessed via the URL and having to do with a computer "session". Similarly, "report designator 718" is a designator, e.g., name or other identifier of the report accessed. The Rejection allegation on page 16 that items 712, 716 and 718 have anything to do with a computer "session" is erroneous, unfounded speculation. These items provide no 35 USC 112 compliant enabling disclosure of "automatically" communicating "application specific **context** information" in "a data field of a URL **separately from session** identification information".

As described above with respect to claims 1, 6, and 14 a "session identifier" identifies a session of computer operation including one or more executable applications (a "session identifier is used by applications 200 and 230 to identify a user initiated session in communicating with manager 250" – Application page 5 lines 29-32, "Specifically the managing application coordinates inactivity timeout operation and maintains and conveys properties between concurrent applications in order to create a smooth user operation session." Application page 4 lines 27-30). This is corroborated in Levergood (a "user is provided with a session identification which allows the user access to the requested file as well as any other files within the present protection domain" – Levergood Abstract). Therefore, "session identification information" is NOT (and is not suggested by) a "date 712 and time 716" associated with requested report data accessed via a URL or a "report designator 718" e.g., name or other identifier of the report accessed. Further, session identification information is not "application specific **context** information" and does NOT support "acquisition from said child application of information associated with a current operational context of said parent application". Though Levergood discloses appending session identification information (SID) to a URL (column 3 line 39), session identification is used for authentication and determining access to documents (a user is provided with a session identification which allows the user access to the requested file as well as any other files within the present protection domain" – Levergood Abstract). Session identification information is not "application specific **context** information" and does NOT support "acquisition from said child application of information associated with a current operational context of said parent application". Cohen with Levergood and De la Huerga also does not suggest the automatic activity of "automatically" communicating "application specific context information" in "a data field of a URL separately from session identification information" together with facilitating automatic authentication to network compatible applications by "communicating said authenticated different user identifier to said **child application**". This provides seamless navigation advantages not shown or suggested in the combined references.

Further, Applicant respectfully submits that incorporating the De la Huerga features in Cohen with Levergood as suggested in the Rejection results in the system burden of requiring a user to initiate at least a second command (e.g., a URL link selection) conveying application specific context information to an application **in addition to** initiating a first command conveying session identification information (e.g., a URL link selection) to the application. These references, in any combination, neither disclose nor suggest the use of a single command to seamlessly achieve this navigation, as described in the present claimed invention. Further the absence of any common problem recognition, advantage identification or other motivation in the three references undermines any suggestion that combining these disparate systems would be obvious to one of ordinary skill in the art. Further, the Rejection fails to provide any showing of how such disparate systems may be combined when each system has features that conflict with systems employed by the other references (in security management, URL format, handshaking etc.).

Consequently it is respectfully submitted that the present invention as claimed in claim 21 is patentable over Cohen in view of Levergood and De la Huerga. Dependent claim 22 is considered to be patentable for the reasons given in connection with claim 21. Therefore, withdrawal of the rejection of claims 21 and 22 under 35 USC 103(a) is respectfully requested.

CLAIM 23

As stated on page 18 of the Rejection, claim 23 is a method claim that mirrors the system of claim 1. Thus the rejection argues that claim 23 is unpatentable for the same reasons given for claim 1. Applicant respectfully submits that claim 23 is in fact patentable for the reasons given above in connection with claim 1. The method of claim 23 includes the activity of "automatically communicating **application specific context** information in a **data field of a URL** separately from session identification information, to a second application of said plurality of network compatible applications in response to a user command to initiate execution of said second application and in response to authentication of said user identification information". Such application specific context information includes a patient identifier or user identifier, for example (Application page 10 lines 35-37). The claimed method advantageously "automatically" communicates "**application specific context** information in a data field of a URL **separately** from session identification information, to a second application of said plurality of network compatible applications" such as a patient identifier "in response to authentication of said user identification information." Further, the "application specific context information" supports "acquisition" from the "second application of information associated with a current operational context of said first application".

Thereby the method enables a user to logon and authenticate with a first application such as a patient census application and gain automatic access to multiple other applications such as a medical laboratory test result application and in response to user authentication with the test result application, be automatically provided with desired test results for the specific patient selected in the first patient administration application (see example described on Application page 5 lines 8-12 and elsewhere in connection with Figure 2). This is done without the user having to re-enter context information (e.g., a patient identifier) by another command following automatic authentication with a second application. This capability is not shown or suggested in Cohen with Levergood and De la Huerga. The combination of automatic authentication to multiple applications together with automatic communication of application specific context information "in response to a user command to initiate execution of said second application and in response to authentication of said user identification information" facilitates user friendly operation and user seamless navigation in a plurality of concurrently operating applications. The method addresses the problems involved in "facilitating user initiation (e.g., logon), operation and termination (e.g., logoff) of multiple Internet applications and in securely passing URL, patient (and user) identification and other information between applications. A managing application is employed to coordinate user operation sessions. Specifically, the managing application coordinates inactivity timeout operation and maintains and conveys properties between concurrent applications in order to **create a smooth user operation session**" (Application page 4 lines 23-31).

The Rejection on page 10 recognizes that Cohen does not disclose the claimed features of "automatically communicating application specific **context** information in a data field of a URL" to a "second application of said plurality of network compatible applications" "in response to authentication of said user identification information." However, Levergood (with Cohen) in column 4 lines 1-18, column 6, lines 58-66 and column 7, lines 15-21 relied on in the Rejection on pages 2-3 and 10 also fails to show or suggest "automatically" communicating "application specific **context** information" (such as a patient identifier) in "a data field of a URL" to a "second application of said plurality of network compatible applications" in "response to authentication of said user identification information." Levergood discloses appending session identification information (SID) to a URL (column 3 line 39) and as indicated in the Rejection, the Levergood SID may incorporate a user identifier (Column 5 lines 56-60). However, the Levergood SID is used for authentication and determining access to documents ("a user is provided with a session identification which allows the user to access to the requested file as well as any other files within the present protection domain" - Levergood Abstract).

Consequently, Levergood with Cohen cannot "automatically" communicate "application specific **context** information" (such as a patient identifier) in "a data field of a URL" to a "second application of said plurality of network compatible applications" in "**response to authentication** of said user identification information". Since the context information relied on in the Rejection is within the SID used to authenticate user access to data it cannot be "automatically" communicated in "**response to authentication"**. Further, the Levergood SID is not "application specific **context** information," as recited in the present claimed invention and does NOT support "acquisition from said second application of information associated with a current operational context of said first application" as recited in the present claimed invention, since it is within the SID used for the entirely different purpose of authentication.

As recognized in the Rejection on page 11, Levergood with Cohen fails to show or suggest "automatically" communicating "application specific **context** information" (such as a patient identifier) in "a data field of a URL **separately from session** identification information". However, contrary to the Rejection statement on page 11, De la Huerga (with or without Levergood and Cohen) also does not show or suggest "automatically" communicating "application specific **context** information" in "a data field of a URL **separately from session** identification information" as recited in the present claimed invention. De la Huerga in column 10 lines 43-59 and Figure 14A shows a URL conveying "application specific **context** information" (a patient identifier) in "a data field of a URL" but does NOT show or suggest a URL conveying **"session** identification information" in a separate data field of the URL. The items relied on in the Rejection in De la Huerga column

10 lines 43-59 have nothing to do with a computer "session" and De la Huerga nowhere even mentions or contemplates "session". De la Huerga column 10 lines 43-59 states "Embedded in this URL address 700 is information regarding the type of data 704, the patient's identification 708, the date 712 and time 716 of the data requested, and a report designator 718". The "date 712 and time 716 of the data requested" are the time and date associated with a report accessed via the URL and have nothing to do with a computer "session". Similarly, "report designator 718" is a designator, e.g., name or other identifier of the report accessed. The Rejection allegation on page 11 that items 712, 716 and 718 have anything to do with a computer "session" is erroneous, unfounded speculation. These items provide no 35 USC 112 compliant enabling disclosure of "automatically" communicating "application specific **context** information" in "a data field of a URL **separately from session** identification information".

Applicant further respectfully submits that the comment in the response to arguments section of the rejection on page 3 **mis-reads** page 5, lines 28-29 of the Application. "The **session** context information comprises a **session** identifier, a hash value, and application specific data" (page 5, lines 28-29). "**Session** context information" is not equivalent to "**application specific** context information." A "session identifier" identifies a session of computer operation including one or more executable applications (a "session identifier is used by applications 200 and 230 to identify a user initiated session in communicating with manager 250" – Application page 5 lines 29-32, "Specifically the managing application coordinates inactivity timeout operation and maintains and conveys properties between concurrent applications in order to create a smooth user operation session." Application page 4 lines 27-30). This is corroborated in Levergood (a "user is provided with a session identification which allows the user access to the requested file as well as any other files within the present protection domain" - Levergood Abstract).

Therefore, "session identification information" is NOT (and is not suggested by) a "date 712 and time 716" associated with requested report data accessed via a URL or a "report designator 718" e.g., name or other identifier of the report accessed. Further, session identification information is not "application specific **context** information" and does NOT support "acquisition from said second application of information associated with a current operational context of said first application". Though Levergood discloses appending session identification information (SID) to a URL (column 3 line 39, and column 6, lines 22-24), session identification is used for authentication and determining access to documents (a user is provided with a session identification which allows the user to access to the requested file as well as any other files within the present protection domain" - Levergood Abstract). Session identification information is not "application specific **context** information" and does NOT support "acquisition from said second application of information associated with a current operational context of said first application". Cohen with Levergood and De la Huerga also does not suggest the automatic feature combination comprising "automatically" communicating "application specific context information" in "a data field of a URL separately from session identification information" together with facilitating automatic authentication to multiple network compatible applications by "communicating an authentication service identifier" and a "corresponding user identifier to a **managing application**". This provides seamless navigation advantages not shown or suggested in the combined references.

Further, Applicant respectfully submits that incorporating the De la Huerga features in Cohen with Levergood as suggested in the Rejection results in the system burden of requiring a user to initiate at least a second command (e.g., a URL link selection) conveying application specific context information to an Application **in addition to** initiating a first command conveying session identification information (e.g., a URL link selection) to the Application. These references, in any combination, neither disclose nor suggest the use of a single command to seamlessly achieve this navigation, as described in the present claimed invention. Further the absence of any common problem recognition, advantage identification or other motivation in the three references undermines any suggestion that combining these disparate systems would be obvious to one of ordinary skill in the art. Further, the Rejection fails to provide any showing of how such disparate systems may be combined when each system has features that conflict with systems employed by the other references (in security management, URL format, handshaking etc.).

Consequently it is respectfully submitted that the present invention as claimed in claim 23 is patentable over Cohen in view of Levergood and De la Huerga. Therefore, withdrawal of the rejection of claim 23 under 35 USC 103(a) is respectfully requested.

VIII CONCLUSION

Claims 1 through 23 are considered patentable because Cohen, Levergood and De la Huerga, either alone or together neither disclose nor suggest "communicating an authentication service identifier and a corresponding user identifier to a managing application, said authentication service identifier identifying an authentication service used to authenticate identification information of said corresponding user" as recited in the present claimed invention. Additionally, Cohen, Levergood and De la Huerga neither disclose nor suggest "automatically communicating application specific context information in a data field of a URL separately from session identification information, to a second application of said plurality of network compatible applications in response to a user command to initiate execution of said second application and in response to authentication of said user identification information" as recited in the present claimed invention. Furthermore, Cohen, Levergood and De la Huerga neither disclose nor suggest "said application specific context information supporting acquisition from said second application of information associated with a current operational context of said first application" as recited in the present claimed invention.

Accordingly it is respectfully submitted that the rejection of Claims 1– 23 should be reversed.

Respectfully submitted,
Siemens Medical Solutions Health Services Corporation

Alexander J. Burke
Reg. No. 40,425

Date: July 10, 2006

Alexander J. Burke
Intellectual Property Department
Siemens Corporation,
170 Wood Avenue South
Iselin, N.J. 08830
Tel. 732 321 3023
Fax 732 321 3030

APPENDIX I - APPEALED CLAIMS

1. (Previously Presented) A system used by a first application for managing user access to at least one of a plurality of network compatible applications, comprising:

an authentication processor for,

receiving user identification information including a user identifier and

initiating authentication of said user identification information using an authentication service; and

at least one communication processor for,

communicating an authentication service identifier and a corresponding user identifier to a managing application, said authentication service identifier identifying an authentication service used to authenticate identification information of said corresponding user and

automatically communicating application specific context information in a data field of a URL separately from session identification information, to a second application of said plurality of network compatible applications in response to a user command to initiate execution of said second application and in response to authentication of said user identification information, said application specific context information supporting acquisition from said second application of information associated with a current operational context of said first application.

2. (Previously Presented) A system used by a first application for managing user access to at least one of a plurality of network compatible applications, comprising:

an authentication processor for,

receiving user identification information including a user identifier and

initiating authentication of said user identification information using an authentication service; and

at least one communication processor for,

communicating an authentication service identifier and a corresponding user identifier to a managing application, said authentication service identifier identifying an authentication service used to authenticate identification information of said corresponding user and

automatically communicating application specific context information in a data field of a URL to a second application of said plurality of network compatible applications in response to a user command to initiate execution of said second application and in response to authentication of said user identification information wherein

said application specific context information comprises at least one of, (a) a user identifier and (b) a patient identifier and

a communication processor of said at least one communication processor encrypts an address portion of said URL and incorporates said encrypted address portion of said URL, together with said address portion of said URL in non-encrypted form, into a single processed URL data string.

3. (Previously Presented) A system according to claim 1, wherein

said application specific context information comprises a patient identifier, a communication processor of said at least one communication processor also communicates a session identifier identifying a user initiated session of operation of said first application to said managing application and

said user identification information includes a password associated with said user identifier.

4. (Previously Presented) A system according to claim 1, wherein

a communication processor of said at least one communication processor communicates said authentication service identifier and said corresponding user identifier to a managing application for compilation of a database.

5. (Original) A system according to claim 4, wherein

said database is accessible by other applications of said plurality of network compatible applications for mapping a non-authenticated user identifier of a participant application to an authenticated and different user identifier of another application.

6. (Previously Presented) A system used for processing user access to network compatible applications, comprising:

an authentication processor for,

receiving authentication service identifier and corresponding user identifier data pairs from at least one of a plurality of applications,

compiling a database using said data pairs,

mapping a non-authenticated user identifier of a second application to an authenticated different user identifier of a first application using said database; and

at least one communication processor for,

communicating said authenticated different user identifier to said second application and automatically communicating application specific context information in a data field of a URL separately from session identification information, to said second application in response to a user command to initiate execution of said second application, said application specific context information supporting acquisition from said second application of information associated with a current operational context of said first application.

7. (Original) A system according to claim 6, wherein

said authentication service identifier identifies an authentication service used to authenticate identification information comprising a user identifier of said corresponding user to provide an authenticated user identifier.

8. (Previously Presented) A system according to claim 6, wherein

said authentication processor performs said mapping using said database by matching an authentication service identifier of said second application with an authentication service identifier of said first application and providing said authenticated different user identifier of said first application as a mapped user identifier.

9. (Previously Presented) A system according to claim 6, including

an input processor for receiving a session identifier identifying a user initiated session of operation wherein

said at least one communication processor encrypts an address portion of said URL and incorporates, said encrypted address portion of said URL, together with said address portion of said URL in non-encrypted form, into a single processed URL data string and provides a key supporting decryption of said encrypted address portion to a destination system.

10. (Original) A system according to claim 6, wherein

said first application is a parent application and said second application is a child application and

said authenticated different user identifier of said first application is used by said second application eliminating the need for said second application to authenticate a user identifier.

11. (Previously Presented) A system according to claim 6, wherein

a communication processor of said at least one communication processor communicates a parameter to said second application, said parameter identifying success or failure of said mapping.

12. (Original) A system according to claim 6, wherein

said authentication processor receives an authentication service identifier and corresponding user identifier data pair from said first application and

said first application is a parent application and said second application is a child application.

13. (Original) A system according to claim 6, wherein

said authentication service identifier employs a predetermined data format for use by said plurality of applications in constraining size of said database.

14. (Previously Presented) A system used for processing user access to Internet compatible applications, comprising:

an authentication processor for,

receiving an authentication service identifier and corresponding user identifier from a parent application, and

mapping a non-authenticated user identifier of a child application to an authenticated different user identifier of said parent application; and

at least one communication processor for,

communicating said authenticated different user identifier to said child application and

automatically communicating application specific context information in a data field of a URL separately from session identification information, to said child application in response to a user command to initiate execution of said child application and in response to communicating said authenticated different user identifier, said application specific context information supporting acquisition from said child application of information associated with a current operational context of said parent application.

15. (Original) A system according to claim 14, wherein

said parent application establishes a session of user operation and

said child application uses said authentication system to participate in said session of user operation.

16. (Original) A system according to claim 14, wherein

said authentication processor compiles a database using data pairs comprising an authentication service identifier and corresponding user identifier and a data pair is received from individual applications of a plurality of concurrently operating Internet compatible applications and

said authentication processor uses said database in mapping said non-authenticated user identifier of said child application to said authenticated different user identifier of said parent application.

17. (Previously Presented) A system according to claim 16, wherein

said authentication processor performs said mapping using said database by matching an authentication service identifier of said child application with an authentication service identifier of said parent application and providing said authenticated different user identifier of said parent application as a mapped user identifier.

18. (Original) A system according to claim 14, wherein

said authentication service identifier identifies an authentication service used to authenticate identification information comprising a user identifier of said corresponding user to provide an authenticated user identifier.

19. (Previously Presented) A system according to claim 14, wherein

said application specific context information comprises a patient identifier and

said authenticated different user identifier of said parent application is used by said child application eliminating the need for said child application to authenticate a user identifier.

20. (Original) A system according to claim 14, wherein

access to said child application by a user is enabled by said child application in response to receiving said authenticated different user identifier without a subsequent re-entry of user identification information via a logon menu.

21. (Previously Presented) A method used for processing user access to Internet compatible applications, comprising the activities of:

receiving an authentication service identifier and corresponding user identifier from a parent application, and

mapping a non-authenticated user identifier of a child application to an authenticated different user identifier of said parent application;

communicating said authenticated different user identifier to said child application; and

automatically communicating application specific context information in a data field of a URL separately from session identification information, to said child application in response to a user command to initiate execution of said child application and in response to communicating said authenticated different user identifier, said application specific context information supporting acquisition from said child application of information associated with a current operational context of said parent application.

22. (Previously Presented) A method according to claim 21, including the activities of

receiving data pairs, comprising an authentication service identifier and corresponding user identifier, from individual applications of a plurality of concurrently operating Internet compatible applications,

compiling a database using said data pairs, and

using said database in mapping said non-authenticated user identifier of said child application to said authenticated different user identifier of said parent application.

23. (Previously Presented) A method used by a first application for managing user access to at least one of a plurality of network compatible applications, comprising the activities of:

receiving user identification information including a user identifier;

initiating authentication of said user identification information using an authentication service;

communicating an authentication service identifier and a corresponding user identifier to a managing application, said authentication service identifier identifying an authentication service used to authenticate identification information of said corresponding user; and

automatically communicating application specific context information in a data field of a URL separately from session identification information, to a second application of said plurality of network compatible applications in response to a user command to initiate execution of said second application and in response to authentication of said user identification information, said application specific context information supporting acquisition from said second application of information associated with a current operational context of said first application.

APPENDIX II - EVIDENCE

Applicant does not rely on any additional evidence other than the arguments submitted hereinabove.

APPENDIX III - RELATED PROCEEDINGS

There is currently a co-pending appeal in related application serial number 09/817,322 wherein a Notice of Appeal has been filed on June 5, 2006. The present application and the application of the co-pending appeal claim priority from the same Provisional Application Serial No. 60/261,148.

A Notice of Appeal was filed in application serial number 09/817,320 on August 15, 2005 and as a result, prosecution was re-opened by Non-Final Office Action on March 9, 2006 followed by a subsequent Notice of Appeal on April 12, 2006. A Request for Continued Examination with a Preliminary Amendment was filed in response thereto on June 12, 2006.

A Notice of Appeal was filed in application serial number 09/817,323 on July 7, 2005 and as a result, prosecution was re-opened by Non-Final Office Action on March 9, 2006. A response to the Non Final Office Action was filed on June 7, 2006.

The present application and application serial numbers 09/817,323 and 09/817,320 claim priority from the same provisional application serial number 60/261,148.

APPENDIX IV - TABLE OF CASES

1. *In re Howard*, 394 F. 2d 869, 157 USPQ 615, 616 (CCPA 1968)

2. 29 AM. Jur 2D Evidence S. 33 (1994)

3. *In re Ahlert*, 424 F. 2d 1088, 1091, 165 USPQ 418, 420 (CCPA 1970)

4. *In re Eynde*, 480 F. 2d 1364, 1370; 178 USPQ 470, 474 (CCPA 1973)

5. *In re Fine*, 5 USPQ 2d 1600, (Fed Cir. 1988)

6. ACS Hospital Systems Inc v. Montefiore Hospital, 221 USPQ 929,933 (Fed. Cir. 1984)

7. *Graham v. John Deere Co.*, 383 U.S. 1, 17, 148 USPQ 459, 467 (CCPA 1966)

8. *Uniroyal, Inc. v. Rudkin-Wiley Corp.*, 837 F.2d 1044, 1051, 5 USPQ2d 1434, 1438 (Fed.Cir. 1988), *cert. denied*, 488 U.S. 825 (1988)

9. *Ashland Oil Inc. v. Delta Resins & Refractories, Inc.*, 776 F.2d 28, 293, 227 USPQ 657, 664 (Fed.Cir. 1985), *cert. denied*, 475 U.S. 1017 (1986)

10. *In re Oetiker*, 977 F2d 1443, 1445, 24 USPQ2d 1443, 1444 (Fed. Cir. 1992)

APPENDIX V - LIST OF REFERENCES

U.S. Pat. No.	**Issued Date**	**102(e) Date**	**Inventors**
6,178,511	January 23, 2001		Cohen et al.
5,708,780	January 13, 1998		Levergood et al.
5,903,889	May 11, 1999		De la Huerga et al.

TABLE OF CONTENTS

ITEMS PAGE

APPENDICES